Ministero delle Infrastrutture e della Mobilità Sostenibili

Dipartimento per la mobilità sostenibile

Direzione Generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione

UN Regulation No. 155

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

Methods and criteria

Version 1.0 – 29/07/2022

TABLE OF CONTENTS

1. SCOPE

This document describes procedures, methods and criteria adopted by the Italian Type Approval Authority and aimed at issuing an approval for a new vehicle type in compliance with UN Regulation No. 155.

Sections applicable to the manufacturer's Cybersecurity Management System (CSMS) audit, including the issue of the relevant certificate, and those applicable to the assessment and testing of the vehicle type under approval are highlighted and well distinguished throughout the document.

This document has been drafted in light of the interpretations adopted by the UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) (see doc. ECE/TRANS/WP.29/2022/61). It will be reviewed on the basis of both the feedback received from other Contracting Parties (UN) and the experience gathered.

2. DEFINITIONS

This document has been drafted taking into account the terms and definitions which are common in the field of type approval regulations, in particular those established by the Agreement concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of Approval for Motor Vehicle Equipment and Parts, done at Geneva on 20 March 1958 (58A Rev.3) and by the UN Regulation No. 155.

In addition, the following terms and definitions apply:

- Commission: the Commission being appointed, through an order from the Director of the Type Approval Authority, to perform the audit aimed at assessing the CSMS compliance;
- Type Approval Authority: Division 3 of the General Directorate for motorised mobility and for services to citizens and enterprises in the field of transport and navigation of the Italian Ministry of sustainable infrastructure and mobility;
- Technical Service: decentralised offices of the Italian Ministry of sustainable infrastructure and mobility entitled "Centro Superiore Ricerche e Prove Autoveicoli e Dispositivi (CSRPAD)" and "Centro Prove Autoveicoli (CPA)" as well as the Technical Service based within Division 3 of the General Directorate for motorised mobility and for services to citizens and enterprises in the field of transport and navigation;
- Certified e-mail address (PEC): the system that enables sending an e-mail with the same legal value of a registered mail with return receipt as established by the Italian Law.

The Type Approval Authority in Italy is established within the Italian Ministry of sustainable infrastructure and mobility. Its reference details are as follows:

Ministero delle Infrastrutture e della Mobilità Sostenibili
Dipartimento per la mobilità sostenibile
Direzione generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione
Divisione 3 – Disciplina tecnica dei veicoli e Autorità di omologazione (Vehicle Type Approvals)
Via Giuseppe Caraci, 36, Roma, Città Metropolitana di Roma, 00157, Lazio, Italia
Email certificata: dg.mot-div3@pec.mit.gov.it
Email: div3.dgmot@mit.gov.it
Telefono: 06/44128473 – 41

3. PROCESSES FOR COMPLIANCE ASSESSMENT

Assessing compliance of the CSMS, as well as issuing of the relevant certificate, is entrusted to the Type Approval Authority.

Assessing compliance of the vehicle type under approval is entrusted to the Technical Service.

3.1 PROCESS DESCRIPTION (FLOWCHART)

3.1.1 ISSUING OF THE CSMS CERTIFICATE

The process for assessing compliance of the Manufacturer’s CMSM can be summarized by the following steps:

- Review of documentation;
- Audit preparation;
- Conducting the on-site audit;
- Drafting the audit report (Annex 4);
- Communication of findings;
- Additional audit (if necessary);
- Issuing the CSMS certificate.

The process is described in detail in the flowchart pictured in Figure 1.

The validity of the CSMS certificate is three years from the issuing date. Within the period of validity, the manufacturer will be subject to surveillance audits at least every twelve months by the Type Approval Authority.

Before the expiry of the three years period of validity the CSMS certificate can be renewed through a repetition of the whole audit process.

The manufacturer is required to inform the Type Approval Authority, through PEC, of any substantial modification to the CSMS that may or may not have potential impacts on the validity of the certificate. The Type Approval Authority, having reviewed the information provided by the manufacturer, will decide whether the modified CSMS is still deemed to comply to the requirements and to the documentation package of the actual approval or, on the other hand, whether it is necessary to conduct a renewal audit. In both cases the Type Approval Authority will reply to the manufacturer, via PEC, in a reasonable time of about one month.

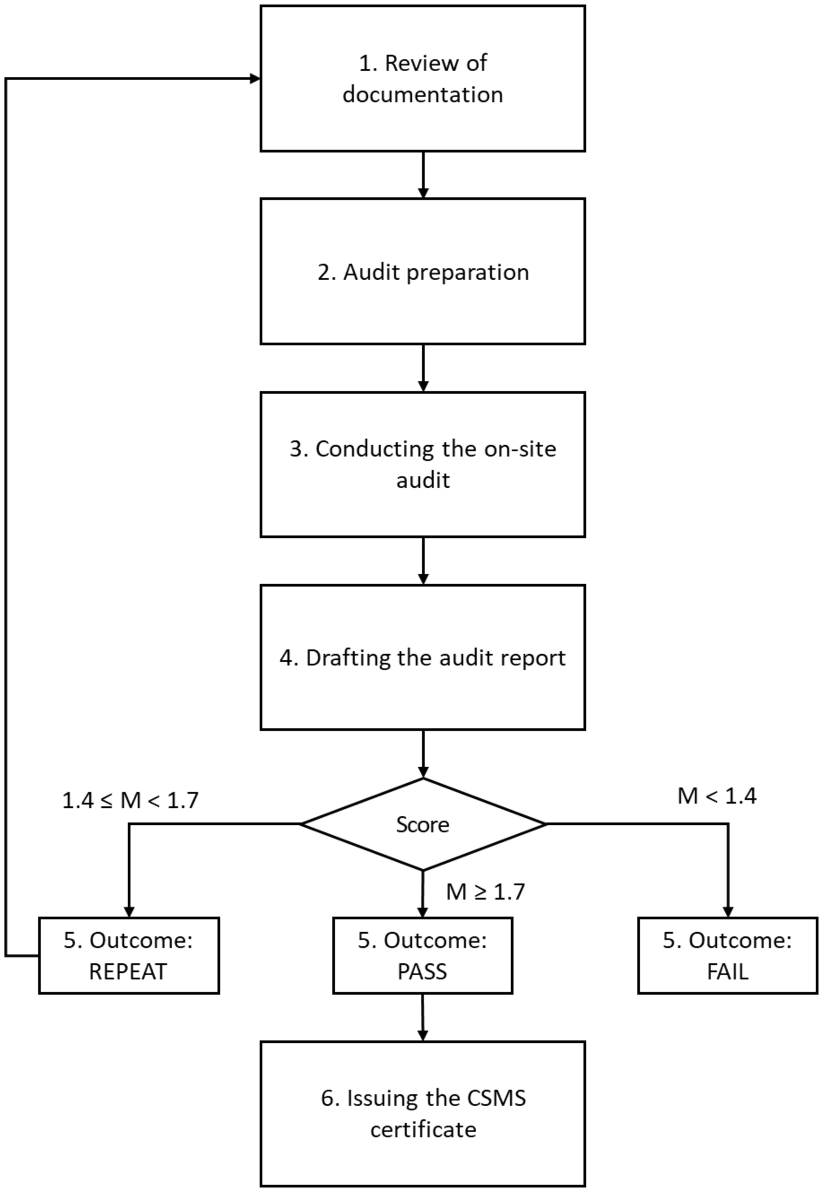
1. Review of documentation
2. Audit preparation
3. Conducting the on-site audit
4. Drafting the audit report
Score
1.4 ≤ M < 1.7
M < 1.4
M ≥ 1.7
5. Outcome: REPEAT
5. Outcome: PASS
5. Outcome: FAIL
6. Issuing the CSMS certificate

Figure 1 – CSMS audit process flowchart

All the documents received by the Type Approval Authority will be evaluated on the basis of general criteria, for example, that they are currently checked, used, accessible, periodically revised, etc.

Such information will be summarized in document sheet as shown in Table 1.

N.	Title	Description	Observations	Evaluation

Table 1 – Document sheet

During the on-site audit all information that could not be gathered through the documents provided by the manufacturer will be registered in an audit sheet as shown in Table 2.

Requirements	**Audit questions**	**Aim/Scope of the question**	**Minimum performance criteria**	**Best practices**	**Additional information / Context**

Table 2 – Audit sheet

3.1.2 VEHCILE TYPE APPROVAL

The process for approving the vehicle type in compliance with UN Regulation No. 155 can be summarized by the following steps:

- Checking the manufacturer's CSMS certificate validity;
- Review of documentation;
- Assessment and testing preparation;
- Conducting the on-site approval assessment;
- Repetition of tests on vehicle type;
- Drafting the approval report (Annex 5);
- Communication of findings;
- Issuing the type approval certificate.

The process is described in detail in the flowchart pictured in Figure 2.

As a first step the Technical Service judges whether the manufacturer's CSMS needs to be complemented or modified or, on the other hand, whether it is fully acceptable in the view of a positive signing of the approval report. If the CSMS needs to be complemented or modified the Technical Service will suspend the type approval process notifying the CSMS adjustment request to both the Type Approval Authority and the manufacturer.

The Technical Service shall check, through appropriate testing either on a vehicle representative of the vehicle type under approval or on its relevant systems or subsystems, that the vehicle manufacturer has implemented the documented cybersecurity protection measures. The testing shall be performed by the Technical Service in cooperation with the vehicle manufacturer through appropriate sampling and, normally, with the assistance of third party experts. The sampling shall be focused on, but not limited to, those risks which have been evaluated as relevant during the risk analysis.

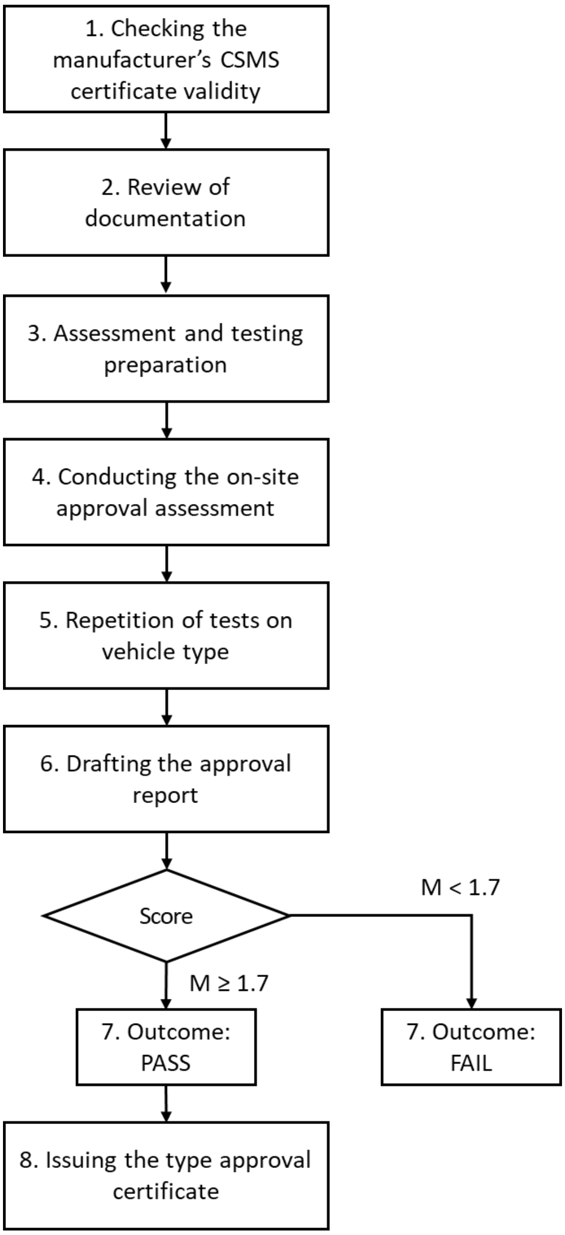
1. Checking the manufacturer's CSMS certificate validity
2. Review of documentation
3. Assessment and testing preparation
4. Conducting the on-site approval assessment
5. Repetition of tests on vehicle type
6. Drafting the approval report
Score
M < 1.7
M ≥ 1.7
7. Outcome: PASS
7. Outcome: FAIL
8. Issuing the type approval certificate

Figure 2 – Type approval process flowchart

The manufacturer is required to inform without delay the Technical Service about any modification to the vehicle type which would bring to a revision or an extension of the type approval. The Technical Service will judge whether a review of documentation is sufficient or whether additional assessment and testing on-site are needed. In the first case the process will result in a type approval revision will be due, while in the second case in a type approval extension.

3.2 PROCESS WORKFLOW

3.2.1 WORKFLOW FOR ISSUING THE CSMS CERTIFICATE

The workflow for conducting the CSMS audit, with indication of the time spent and the resources involved for each step of the process, is described in detail in Table 3.

CSMS audit step	Duration (max)	Roles involved
1. Review of documentation*	6 days	Chair of the Commission Cybersecurity expert Management systems expert
2. Audit preparation*	5 days	Chair of the Commission Cybersecurity expert
3. Conducting the on-site audit*	5 days	Chair of the Commission Cybersecurity expert Management systems expert
4. Drafting the audit report*	2 days	Chair of the Commission Management systems expert
5. Communication of findings	1 day	Chair of the Commission
6. Issuing the CSMS certificate	2 days	Type Approval Authority manager
* In case the outcome is positive with reservations, the process will be repeated only once focusing on the elements that drew the attention of the Commission during the audit		

Table 3 – CSMS audit workflow

3.2.2 WORKFLOW FOR VEHICLE TYPE APPROVAL

The workflow for the type approval activities, with indication of the time spent and the resources involved for each step of the process, is described in detail in Table 4.

Type approval step	Duration (max)	Roles involved
1. Checking the manufacturer's CSMS certificate validity	2 days	Technical Service Manager Cybersecurity expert
2. Review of documentation	3 days	Technical Service Manager Cybersecurity expert Type approval expert
3. Assessment and testing preparation	2 days	Technical Service Manager Cybersecurity expert
4. Conducting the on-site approval assessment	3 days	Technical Service Manager Cybersecurity expert Type approval expert
5. Repetition of tests on vehicle type	2 days	Technical Service Manager Cybersecurity expert Type approval expert
6. Drafting the approval report	2 days	Technical Service Manager Type approval expert
7. Communication of findings	1 day	Technical Service Manager
8. Issuing the type approval certificate	2 days	Type Approval Authority manager

Table 4 – Type approval workflow

3.3 CRITERIA FOR COMPLIANCE ASSESSMENT

3.3.1 CRITERIA FOR ISSUING THE CSMS CERTIFICATE

The evaluation of the findings from the audit of manufacturer's CSMS, applicable to each item of the checklist defined in par. 6.3., is based on a three level scoring system (2/1/0). The outcome of the evaluation is based on the calculation of the average, M, of the points obtained.

When either M < 1,4 or even only a 0 score is present, the outcome of the evaluation is negative (Fail).

When both 1,4≤ M < 1,7 and no 0 score is present, the outcome of the evaluation is positive with reservations. In that case the Technical Service will require that the manufacturer implement the necessary corrective actions and will schedule an additional audit as shown in the flowchart in Figure 1 (Repeat).

When both M ≥ 1,7 and no 0 score is present, the result of the evaluation is positive (Pass).

3.3.2 CRITERIA FOR ISSUING VEHICLE TYPE APPROVAL

The evaluation of the findings from the assessment of the vehicle type, applicable to each item of the checklist defined in par. 7.1., is based on a three level scoring system (2/1/0). The outcome of the evaluation is based on the calculation of the average, M, of the points obtained.

When either M < 1,7 or even only a 0 score is present, the outcome of the evaluation is negative (Fail).

When both M ≥ 1,7 and no 0 score is present, the result of the evaluation is positive (Pass).

To a positive evaluation of the assessment shall also correspond a satisfactory result of the physical tests on the vehicle type that have been repeated during the on-site testing for type approval as described in par. 7.2.

4. PERSONNEL QUALIFICATION

4.1 AUDITING AND ASSESSMENT TEAMS SETUP

4.1.1 COMMISSION FOR THE CSMS AUDIT

The Commission for the CSMS audit will be identified by the Type Approval Authority and will be made of:

- Chair of the Commission and chief of procedings;
- Cybersecurity expert;
- Management systems expert.

The Commission setup, with the description of the assignments given to each of its members, is described in detail in Table 5.

If a component of the Commission fulfills the requirements given in par. 4.2., Table 7, the same person can be assigned with different roles and the total number of the personnel in the Commission can be reduced to 2.

Role	Number	Responsibilities
Chair of the Commission	1	He/She is in charge for planning and conducting the audit. Decides on the outcome of the audit.
Cybersecurity expert	1	He/She supports the Commission with specific know-how in the field of cybersecurity.
Management systems expert	1	He/She supports the Commission with a broad range of competence in the field of management systems and relevant processes.

Table 5 – Commission setup

4.1.2 TECHNICAL SERVICE STAFF FOR VEHICLE TYPE APPROVAL

The Technical Services entitled to conduct the assessment and testing for type approval belong to category B as defined by the 1958 Agreement Rev.3, schedule 2, Part 1, par. 1.3., letter B), and shall prove they have identified, within their technical personnel, properly educated and trained resources with the necessary requisites of competence and professional experience.

The personnel in charge with the assessment and testing for type approval will be identified by the Technical Service and will be made of:

- Technical Service manager and chief of procedings;
- Cybersecurity expert;
- Type approval expert.

The Technical Service team setup, with the description of the assignments given to each of its members, is described in detail in Table 6.

If a component of the team fulfills the requirements given in par. 4.2., Table 7, the same person can be assigned with different roles and the total number of the personnel in the team can be reduced to 2.

Role	Number	Responsibilities
Technical Service manager	1	He/She is in charge for planning and conducting the assessment. Decides on the repetition of tests and on the outcome of the assessment.
Cybersecurity expert	1	He/She supports the chief of proceedings with specific know-how in the field of cybersecurity.
Type approval expert	1	He/She supports the chief of proceedings with administrative and technical knowledge on type approval processes.

Table 6 – Technical Service setup

4.1.3 EXCHANGE OF EXPERIENCE

In order to maintain and, if possible, increase knowledge in the field for personnel involved in the various processes, the Approval Authority will promote the exchange of experience, via communication platform (e.g. Teams) among the personnel involved in order to refine the procedures adopted and will promote specific refresher courses as appropriate.

4.2 PROFESSIONAL REQUIREMENTS

Table 7 provides an indication of the minimum qualification requirements, with regard to education degrees, training and professional experience, that need to be complied with by each component of the Commission and of the Technical Service team.

Role	Education degrees	Professional experience	Specific training
Chief of proceedings	Master’s degree in engineering or architecture (or equivalent titles) and licence to lawfully practice the profession	5 years of activity within a Technical Service Excellent relational, decisional and leadership skills	Specialized training course (40 hours min.) on UN Reg. No. 155 and ISO/SAE 21434
Cybersecurity expert	Master’s degree in engineering or architecture (or equivalent titles) and licence to lawfully practice the profession	5 years of activity within a Technical Service In-depth knowledge of UN Reg. No. 155 and of cybersecurity standards	Specialized training course (40 hours min.) on UN Reg. No. 155 and ISO/SAE 21434
Management systems expert	Master’s degree in engineering or architecture (or equivalent titles) and licence to lawfully practice the profession	1 year of activity within a Technical Service Proven experience in conducting CoP audits	
Type approval expert	Master’s degree in engineering or architecture (or equivalent titles) and licence to lawfully practice the profession	1 year of activity within a Technical Service Proven experience in conducting type approval assessments and testing	

Table 7 – Minimum qualification requirements

5. REQUIRED DOCUMENTATION

5.1 DOCUMENTS FOLDER

To prepare for the CSMS audit and for the approval of the vehicle type, the manufacturer shall provide to the Technical Service a documents folder including the reference to all documents and registrations helpful as a proof of compliance to the requirements established by UN Regulation No. 155.

The documents folder will be structured so as to perfectly integrate itself within the company processes, therefore its structure may sensibly differ from one manufacturer to another.

In order to facilitate the assessment by the Technical Service that all the documents and registrations useful as a proof of compliance have been made available from the manufacturer, the documents folder shall be complemented, in a separate annex, with a compliance matrix drafted following the criteria given in par. 5.2.

5.1.1 CSMS DOCUMENTS FOLDER

A non-comprehensive list of documents and registrations that the manufacturer may make reference to in the documents folder and may provide to the Commission, on request, during the on-site audit is shown in Table 8.

The manufacturer, should it be an entitled holder of a previous CSMS certificate having been granted by another Type Approval Authority, is allowed to provide it as a complement to the documents folder.

Requirement	Description	Evaluation criteria	Requested evidence
6.2.	An application for a Certificate of Compliance for Cyber Security Management System shall be submitted by the vehicle manufacturer or by their duly accredited representative.	Administrative analysis and evaluation of applications, in compliance with Annex 2, received via PEC	For applications via PEC a digital signature validated by the Authority is required
6.3.1	Documents describing the Cyber Security Management System.	Technical analysis and evaluation of the documents attached to the application as requested by Annex 2	Approval of data provided by the manufacturer which are deemed to be exhaustive in describing the CSMS
7.2.2.1 7.2.2.2 7.2.2.3 7.2.2.4 7.2.2.5	Documents provided by the manufacturer and necessary to evaluate processes and methods implemented within the CSMS.	Technical analysis and evaluation of the documentation provided by the manufacturer in compliance to Table 11 under par. 6.3. “Interpretation of requirements for the CSMS audit”	Documents review focused on manufacturer’s processes and, if necessary, check of the means used by the manufacturer to keep track of evidence

Table 8 – Illustrative list of documents useful for the CSMS audit

5.1.2 VEHICLE TYPE DOCUMENTS FOLDER

A non-comprehensive list of documents and registrations that the manufacturer may make reference to in the documents folder and may provide to the Technical Service, on request, during the approval of the vehicle type is shown in Table 9.

Requirement	Description	Evaluation criteria	Requested evidence
3.1	The application for approval of a vehicle type with regard to cyber security shall be submitted by the vehicle manufacturer or by their duly accredited representative.	Administrative analysis and evaluation of applications, in compliance with Annex 3, received via PEC	Applications shall be signed digitally and submitted via PEC
3.2.1	A description of the vehicle type with regard to the items specified in Annex 1 to this Regulation.	Technical analysis and evaluation of the documents attached to the application as requested by Annex 3	Approval of data provided by the manufacturer which are deemed to be exhaustive in

			describing the vehicle type
3.2.2	In cases where information is shown to be covered by intellectual property rights or to constitute specific know-how of the manufacturer or of their suppliers, the manufacturer or their suppliers shall make available sufficient information to enable the checks referred to in this Regulation to be made properly. Such information shall be treated on a confidential basis.	Analysis and evaluation of the justifications provided by the manufacturer on the confidentiality of data covered by IPR or which are covered by industrial secret and which cannot be shared without obtaining a prior consent from the manufacturer	Documented evaluation of manufacturer’s declarations
7.3.2. 7.3.3. 7.3.4. 7.3.5. 7.3.6. 7.3.7. 7.3.8.	Documents provided by the manufacturer and necessary to evaluate processes and methods implemented to ensure cybersecurity of the vehicle type under approval.	Technical analysis and evaluation of the documentation provided by the manufacturer in compliance to Table 12 under par. 7.1. “Interpretation of requirements for the approval of the vehicle type”	Documents review focused on manufacturer’s processes and, if necessary, check of the means used by the manufacturer to keep track of evidence
7.4.1.	The vehicle manufacturer shall report at least once a year, or more frequently if relevant, to the Approval Authority or the Technical Service the outcome of their monitoring activities, as defined in paragraph 7.2.2.2.(g)), this shall include relevant information on new cyber-attacks. The vehicle manufacturer shall also report and confirm to the Approval Authority or the Technical Service that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken.	Analysis and evaluation of the reports on their monitoring activities submitted by the manufacturer through PEC	Documented evaluation of manufacturer’s reports Check of the means used by the manufacturer to keep track of evidence

Table 9 – Illustrative list of documents useful for the type approval

5.2 COMPLIANCE MATRIX

The compliance matrix is used by each manufacturer to prove to the Technical Service that all the requirements of UN Regulation No. 155 applicable to the CSMS and to the vehicle type under approval have been fulfilled through their appropriate integration within the company processes.

Annex 1 shows an example of a possible structure of the compliance matrix.

6. SPECIFIC CRITERIA FOR THE CSMS AUDIT

6.1 ON-SITE AUDIT

The CSMS is conducted on-site. In this way access to strictly confidential documents which cannot be shared with the Type Approval Authority by other means can be granted and the effective implementation of the company processes by the organization can be assessed live.

In case several sites/plants are involved in the CSMS processes, the Commission and the manufacturer will decide in which site (it might be more than one) is more convenient to conduct the audit.

6.2 REFERENCE STANDARDS

No compulsory certification is requested to the manufacturer to be eligible for the CSMS auditing. Nevertheless, the manufacturer shall provide to the Commission all the relevant information regarding potential certificates, valid at the time of the application, as a proof of compliance of the organization to recognised standards in the field of management systems.

A non-comprehensive list of the reference standards in the field of management systems which can be helpful during the CSMS audit is shown in Table 10.

Reference/Number	Title
ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements
ISO/SAE 21434:2021	Road vehicles — Cybersecurity engineering
SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
ISO 26262 series	Road vehicles — Functional safety
ISO 9001:2015	Quality management systems — Requirements

Table 10 – Illustrative list of standards useful for CSMS audit

6.3 INTERPRETATION OF REQUIREMENTS FOR THE CSMS AUDIT

Table 11 describes the verification process for the requirements of UN Regulation No. 155 which are relevant for the CSMS.

To each and every requirement a score will be assigned (2/1/0) during the audit, as described in par. 3.3.1.

UN R155	Requirement	Interpretation with ref. to ECE/TRANS/WP.29/2022/61	Examples of documents/proofs which may be provided (with ref. to ECE/TRANS/WP.29/2022/61)
7.1.1.	The vehicle manufacturer has processes that verify that the requirements of this Regulation shall not restrict provisions or requirements of other UN regulations	The requirements of this Regulation shall not restrict provisions or requirements of other UN Regulations as well as national or regional legislations as described in points 1.3. and 1.4. of the scope of this Regulation.	
7.2.1	The Manufacturer has in place a business organization, responsibilities and areas of responsibility of relevant personnel, appropriate resources and measures, documented control plans, test execution instructions, report management, results verification, and	The intention of this requirement is that the Technical Service or Approval Authority shall verify that: (a) The vehicle manufacturer has a CSMS; (b) The presented CSMS complies to the requirements listed below in this regulation.	The following standards may be applicable: (e) ISO/SAE 21434 may be used as the basis for evidencing and evaluating the CSMS. Clauses 5 "Organizational cybersecurity management", 6 "Project dependent cybersecurity management",

	plan control to verify that the cybersecurity management system (CSMS) is in compliance with the regulation	For this requirement the focus is on the manufacturer's processes and assessing if they are in place, in order to get an overview of the capability of the manufacturer to fulfil the requirements of the CSMS. The follow clarifications should be noted: (c) The CSMS may be a part of the organization's Quality Management System or be independent of it; (d) If the CSMS is part of the organization's QMS it should be clearly identifiable.	and 8 "Continual cybersecurity activities" could be used to evaluate the CSMS in general; (f) ISO 18045, ISO 15408, ISO 27000 series, ISO 31000 series may be applicable to relevant parts of the CSMS.
7.2.2.1.	The vehicle manufacturer has a Cyber Security Management System which applies to the following phases: (a) development phase, (b) production phase, (c) post-production phase	The intention of this requirement is that the cybersecurity management system should be able to demonstrate how a manufacturer will handle cybersecurity during the operational life of vehicles produced under a vehicle type. This includes evidencing that there are procedures and processes implemented to cover the three phases. The different phases of the lifecycle may have specific activities to be performed in each of them. 7.2.2.1. describes the different phases of the vehicle type to be considered in the CSMS and 7.2.2.2. applies to all these phases if not stated otherwise. The phases also apply to 7.2.2.4. The CSMS may include active and/or reactive processes or procedures covering the end of support for a vehicle type and how this is implemented or triggered. It may include the possibility to disconnect non-mandatory functions/systems and under what conditions this might happen. The operational life (use phase) of an individual vehicle will commence during the production phase of the vehicle type. It will end during either the production phase or post-production phase of the vehicle type.	The following standards may be applicable: (a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating the required phases of the CSMS. Clauses 9 "Concept ", 10 "Product development", and 11 "Cybersecurity validation" could be used to evaluate the Development phase of the CSMS. Clause 12 "Production" could be used to evaluate the Production phase of the CSMS. Clauses 8 "Continual cybersecurity activities", 13 "Operations and maintenance", and 14 "End of cybersecurity support and decommissioning" could be used to evaluate the post-production phase of the CSMS; (b) Other standards that may be applicable to 7.2.2. and its sub-requirements include: ISO 18045, ISO 15408, ISO 27000 series, ISO 31000 series.
7.2.2.2.(a)	The vehicle manufacturer has processes used within the manufacturer's organization to manage cyber security	The aim of this requirement is to ensure that the organization has processes to manage the implementation of the CSMS. Its scope is limited to processes that are relevant for the cyber security of the vehicle types and not other aspects of the organization. For example, the scope of this requirement is not intended to cover the entire Information Security Management System of an organization. The requirement should be considered unfulfilled if one of the following statements is true 1. Processes are absent or incomplete. 2. Processes are not applied universally or consistently. 3. Processes are often or routinely circumvented to achieve business objectives. 4. The vehicle manufacturer's security governance and risk management approach has no bearing on its processes. 5. System security is totally reliant on users' careful and consistent application of manual security processes. 6. Processes have not been reviewed in response to major changes (e.g. technology or regulatory framework), or within a suitable period. 7. Processes are not readily available to staff, too detailed to remember, or too hard to understand.	The following could be used to show the range of activities performed by the manufacturer to manage the cyber security of the development, production and post-production phases of a vehicle type: (a) Organizational structure used to address cyber security; (b) Roles and Responsibilities regarding cybersecurity management incl. accountability. Examples of documents/evidence that could be provided (c) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-05-01], [RQ-05-02], [RQ-05-06], [RQ-05-07]; (d) BSI PAS 1885 could be used to help evidence this requirement. National certification schemes, like the UK Cyber Essentials, could be used to evidence a manufacturer's organizational processes.

		The requirement may be considered fulfilled if all the following statements are true 1. The vehicle manufacturer fully documents its overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is integrated and embedded throughout these processes and key performance indicators are reported to its executive management. 2. The vehicle manufacturer's processes are developed to be practical, usable and appropriate for its policies and technologies. 3. Processes that rely on user behaviour are practical, appropriate and achievable. 4. The vehicle manufacturer reviews and updates processes at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a major cyber security incident. 5. Any changes to the essential function or the threat it faces triggers a review of processes. 6. The vehicle manufacturer's systems are designed so that they are, and remain, secure even when user security policies and processes are not always followed. For such claim a justification should be provided.	
7.2.2.2.(b)	The vehicle manufacturer has processes used for the identification of risks to vehicle types; within these processes, the threats in Annex 5, Part A of the Regulation and other relevant threats are considered	The aim of this requirement is for a manufacturer to demonstrate the processes and procedures they use to identify risks to vehicle types. Processes implemented should consider all probable sources of risk. This shall include risks identified Annex 5 of the Cyber Security Regulation e.g. risks arising from connected services or dependencies external to the vehicle. The processes may consider: (d) Identification the relevance of a system to cybersecurity; (e) Description of the overall system with respect to: (i) Definition of the system/function; (ii) Boundaries and interactions with other systems; (iii) Architecture; (iv) Environment of operation of the system (context, constraints and assumptions). (f) Identification of assets; (g) Identification of threats; (h) Identification of vulnerabilities. The requirement should be considered unfulfilled if one of the following statements is true 1. Risk identification is not based on a clearly defined set of assumptions. 2. Risk identification for vehicle types are a "one-off" activity (or not done at all). 3. Vehicle types are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments). The requirement may be considered fulfilled if all the following statements are true 1. The vehicle manufacturer's organisational process ensures that security risks to vehicle types are identified, analysed, prioritised, and managed. 2. The vehicle manufacturer's approach to risk is focused on the possibility of adverse	Sources for risk identification may be stated. These may include: (a) Vulnerability/ Threats sharing platforms; (b) Lessons learned regarding risks and vulnerabilities. The following standards may be applicable: (c) ISO/SAE 21434, especially based on [RQ-15-01], [RQ-15-02] , [RQ-15-03], [RQ-15-08].

		impact to its vehicle types, leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of its networks and systems. 3. The vehicle manufacturer's risk identification is based on a clearly understood set of assumptions, informed by an up-to-date understanding of security threats to its vehicle types and its sector. 4. The vehicle manufacturer's risk identification is informed by an understanding of the vulnerabilities in its vehicle types. 5. The vehicle manufacturer performs detailed threat analysis and understand how this applies to your its organisation in the context of the threat to its vehicle types and its sector.	
7.2.2.2.(c)	The vehicle manufacturer has processes used for the assessment, categorization and treatment of the risks identified	The aim of this requirement is that the manufacturer demonstrates the processes and rules they use to assess, categorize and treat risks identified. The processes may consider: (c) Assessing the associated impact related to the risks identified in requirement 7.2.2.2. b); (d) Identification of potential attack paths related to risks identified in requirement 7.2.2.2. b); (e) Determination of feasibility/likelihood of attack for every attack paths identified above; (f) Calculation and categorization of risks; (g) Treatment options of those identified and categorized risks. The requirement should be considered unfulfilled if one of the following statements is true 1. Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner. 2. Security requirements and mitigation techniques are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of vehicle types. 3. Only certain domains or types of asset are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT). 4. Inventories of assets relevant to vehicle types are incomplete, non-existent, or inadequately detailed. 5. Asset inventories are neglected and out of date. 6. Systems are assessed in isolation, without consideration of dependencies and interactions with other systems (e.g. interactions between IT and OT environments). 7. Risk assessments are not based on a clearly defined set of assumptions. 8. Risk assessments for vehicle types are a "one-off" activity (or not done at all). The requirement may be considered fulfilled if all the following statements are true 1. The output from the vehicle manufacturer's risk management process is a clear set of security requirements that will address the risks in line with its organisational approach to security.	The following standards may be applicable: (a) ISO/SAE 21434, especially based on [RQ-15-15], [RQ-15-16], [RQ-15-04]. [RQ-15-05], [RQ-15-10], [RQ-15-17], [RQ-09-05], [RQ-09-06]; (b) BSI PAS 11281:2018 may be applicable for the consideration of safety and security.

		2. All assets relevant to the secure operation of its vehicle types are identified and inventoried (at a suitable level of detail). 3. The inventory is kept up-to-date. 4. Dependencies on supporting infrastructure are recognised and recorded. 5. The vehicle manufacturer has prioritised assets according to their importance to the operation of its vehicle types. 6. The vehicle manufacturer's risk identification is based on a clearly understood set of assumptions, informed by an up-to-date understanding of security threats to its vehicle types and its sector. 7. The vehicle manufacturer's risk identification is informed by an understanding of the vulnerabilities in its vehicle types. 8. The manufacturer can demonstrate the effectiveness and repeatability of their processes for their categorisation and treatment of risk.	
7.2.2.2.(d)	The vehicle manufacturer has processes in place to verify that the risks identified are appropriately managed	The aim of this requirement is that the manufacturer demonstrates the processes and rules they use to decide how to manage the risks. This can include the decision criteria for risk treatment, e.g. the process for selecting what controls to implement and when to accept a risk. The results of the process for risks identification and assessment should feed into selecting the appropriate treatment category options to address those risks. The outcome of this process should be that the residual risk (risks remaining after treatment) is within the manufacturer's stated tolerance of risks (i.e. within stated acceptable limits). Mitigations identified in Annex 5 of the Cyber Security Regulation shall be considered in the processes. The processes may consider: (c) Appropriate and proportional risk treatment methodologies; (d) Treatment of critical elements (with safety and environment) to ensure the risks to them are appropriately mitigated and proportionately based on the safety or environmental goal of dependent vehicle systems; (e) Ensuring the residual risk remains within acceptable limits for components or the overall vehicle type; (f) Detailing any cases where the organization would accept justification for non-adherence to their stated risk tolerance. The requirement should be considered unfulfilled if one of the following statements is true 1. The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes. 2. There is no systemic process in place to ensure that identified security risks are managed effectively. 3. Risks remain unresolved on a register for prolonged periods of time awaiting senior decision-making or resource allocation to resolve. The requirement may be considered fulfilled if all the following statements are true	The following standards may be applicable: (a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-07], [RQ-09-11], and [RQ-11-01]; (b) ISO 31000 may be applicable if adapted for product related risks.

		1. Significant conclusions reached in the course of the vehicle manufacturer's risk management process are communicated to key security decision-makers and accountable individuals. 2. The effectiveness of the vehicle manufacturer's risk management process is reviewed periodically, and improvements made as required.	
7.2.2.2.(e)	The vehicle manufacturer has processes used for testing the cyber security of a vehicle type	The aim of this requirement is to ensure the manufacturer has appropriate capabilities and processes for testing the vehicle type throughout its development and production phases. Testing processes in the production phase may be different to the ones used during the development phase. The processes may consider: Development Phase: (c) Organization specific rules for testing during development; (d) Processes for creation and execution of test strategies; (e) Processes for cybersecurity testing planning; (f) Processes for cybersecurity system design testing; (g) Processes for cybersecurity software unit testing; (h) Processes for cybersecurity hardware testing; (i) Processes for cybersecurity integration testing; (j) Processes for documentation of the results of testing; (k) Processes for handling vulnerabilities identified during testing; (l) Justification and requirements for cybersecurity tests, like Functional (requirement-based, positive and negative) testing, Interface testing, Penetration testing, Vulnerability scanning, Fuzz testing but not limited to the same. Production Phase: (m) Processes for testing to ensure the produced system has the cybersecurity requirements, controls and capabilities outlined in the production plan; (n) Processes for testing to ensure the produced item meets the cybersecurity specifications which are in accordance with the system in the development phase; (o) Processes for testing to assure that cybersecurity controls and configuration as cybersecurity specifications are enabled in the produced item; (p) Processes for documenting the test results and findings handling. The requirement should be considered unfulfilled if one of the following statements is true 1. A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value. 2. Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments. 3. Assurance is assumed because there have been no known problems to date.	The following standards may be applicable: (a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on, , [RQ-10-09], [RQ-10-10], [RQ-11-01], ; (b) BSI PAS 11281:2018 may be utilised for considering the interaction of safety and security and processes for evidencing security outcomes are met.

		The requirement may be considered fulfilled if all the following statements are true 1. The vehicle manufacturer validates that the security measures in place to protect systems are effective and remain effective until the end-of-life of all vehicles under the vehicle types for which they are needed. 2. The vehicle manufacturer understands the assurance methods available to it and chooses appropriate methods to gain confidence in the security of vehicle types. 3. The vehicle manufacturer’s confidence in the security as it relates to its technology, people, and processes can be justified to, and verified by, a third party. 4. Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way. 5. The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.	
7.2.2.2.(f)	The vehicle manufacturer has processes used for ensuring that the risk assessment is kept current	The aim of this requirement is to ensure the risk assessment is kept current. This should include processes to identify if the risks to a vehicle type have changed and how this will be considered within the risk assessment. It is noted that requirements 7.2.2.2. parts f) to h) may have overlaps in terms of the processes used and therefore the same evidence may be applicable to demonstrating that these requirements are met. The requirement should be considered unfulfilled if one of the following statements is true 1. No processes are in place which require the risk assessment to be updated. The requirement may be considered fulfilled if all the following statements are true 1. The vehicle manufacturer conducts risk assessments when significant events potentially affect vehicle types, such as replacing a system or a change in the cyber security threat. 2. The vehicle manufacturer’s risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to vehicle types, change of use and new threat information.	Sources for risk identification may be stated. These may include: (a) Vulnerability/ Threats sharing platforms; (b) Lessons learned regarding risks and vulnerabilities; (c) Conferences. (d) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on[RQ-08-07] [RQ-06-09]., [RQ-07-06].
7.2.2.2.(g)	The vehicle manufacturer has processes used to monitor for, detect and respond to cyberattacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified	The aim of this requirement is to ensure that the manufacturer has processes to monitor for cyber-attacks, threats or vulnerability to vehicles that the manufacturer has had type approved, i.e. are in the post-production or production phase, and that they have established processes that would permit them to respond in an appropriate and timely manner. It is noted that requirements 7.2.2.2. parts f) to h) may have overlaps in terms of the processes used and therefore the same evidence may be applicable to demonstrating that these requirements are met. The requirement should be considered unfulfilled if one of the following statements is true 1. The vehicle manufacturer has no sources of threat intelligence.	The following standards may be applicable: (a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-08-01], [RQ-08-02]. [RQ-08-03], [RQ-08-04], [RQ-08-05], [RQ-08-07], [RQ-08-08], [RQ-07-06], , [RC-07-08], [RQ-13-01], and [RQ-13-02]. The following could be used to evidence the processes used: (b) Cyber security monitoring processes for post-production vehicles. This may include processes that will collect information that may or may not be pertinent to the manufacturer’s vehicle/system; (c) Cyber security information assessment processes. These will be processes for the identification of the relevance of the information collected

		2. The vehicle manufacturer does not apply updates in a timely way, after receiving them. 3. The vehicle manufacturer does not evaluate the usefulness of its threat intelligence or share feedback with providers, authorised aftermarket service providers or other users. 4. There are no staff who perform a monitoring function. 5. Monitoring staff do not have the correct specialist skills. 6. Monitoring staff are not capable of reporting against governance requirements. 7. Security alerts relating to vehicle types are not prioritised. The requirement may be considered fulfilled if all the following statements are true 1. Data relating to the security and operation of vehicle types is collected. 2. Alerts from third parties are investigated, and action taken. 3. Some logging datasets can be easily queried with search tools to aid investigations. 4. The resolution of alerts to an asset or system is performed regularly. 5. Security alerts relating to vehicle types are prioritised. 6. The vehicle manufacturer applies updates in a timely way. 7. The vehicle manufacturer has processes to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities which are relevant to its business needs, or specific threats in its sector. 8. The vehicle manufacturer knows how effective its processes are (e.g. by tracking how they helps it identify security problems). 9. Monitoring staff have appropriate investigative skills and a basic understanding of the data they need to work with. 10. Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers). 11. The vehicle manufacturer successfully demonstrates the processes to evaluate whether the cyber security measures implemented are robust enough to conclude whether they are still effective.	with respect to the system/vehicle of the manufacturer; (d) Processes for risk determination/assessment for the relevant information; (e) Incident response procedures for both vehicles already registered and yet to be registered of the vehicle types covered by the CSMS, which may include evidence of procedures for: (i) Interaction with authorities; (ii) Identified or stated triggers that would lead to an escalation or action; (iii) Determining what response options might be implemented for which condition; (iv) Handling any dependencies and interactions with suppliers. (f) Evidence that the response procedures would work, for example through exercising and verification that planning assumptions remain valid under test.
7.2.2.2.(h)	The vehicle manufacturer has processes used to provide relevant data to support analysis of attempted or successful cyber-attacks	The intention of this requirement is to ensure that a process has been established to provide the data required for analysis and associated responsibilities for handling the data and analysis.	(a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-08-03], [RQ-08-04]. The following could be used to evidence the processes used: (b) Procedure for implementing Security Incident Response Team activities (incidents); (c) Field monitoring (obtaining information on incidents and vulnerabilities); (d) Procedure when an incident occurs (including an overview of what information is passed to the analyst in what steps); (e) Procedure when a vulnerability is discovered (including an overview of what information is passed to the analyst in what steps).
7.2.2.3.	The vehicle manufacturer has processes used within their Cyber Security	The intention of this requirement is to ensure that after the identified risks have been	ISO/SAE 21434 can be used as the basis for evidencing the required processes,

	Management System that ensure that, based on categorization referred to paragraphs 7.2.2.2.(c) and 7.2.2.2.(g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe	classified, a process has been established to determine the response time limit based on the classification results. It is necessary to set the response deadline by processes such as triage and explain the monitoring process to see if it is executed within the deadline. The timeframes provided by the manufacturers should be able to be justified and explained. There may be a set of timeframes covering different possible situations. This should include timeframes for deciding and implementing possible reactions or responses.	especially based on [RQ-08-07] and [RQ-08-08]. The following could be used to evidence the processes used: (a) Procedure for implementing cyber security incident response activities, including: (i) Field monitoring (obtaining information on incidents and vulnerabilities); (ii) Procedure for incident handling, including how the timeframe to respond is determined; (iii) Procedures for discovering vulnerabilities. (b) Demonstration of how the procedures are implemented.
7.2.2.4.	The vehicle manufacturer has processes used within their Cyber Security Management System that ensure that the monitoring referred to in paragraph 7.2.2.2 (g) shall be continual, include vehicles after first registration and is capable to analyse and detect cyber threats, vulnerabilities and cyberattacks from vehicle data and vehicle logs	The intention of this requirement is to ensure that processes of monitoring for cyber-attacks, cyber threats and vulnerabilities on vehicle types are continual and apply to all registered vehicles of the manufacturer that fall within the scope of their Cyber Security Management System and use: (a) the information on monitoring acquired in accordance with 7.3.7. in addition to other sources of information on monitoring acquired in accordance with 7.2.2.2. (g) (such as social media). It is noted that paragraph 1.3., and compliancy with data privacy laws, are particularly relevant to this requirement.	ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on 8.3 "Cybersecurity Monitoring", 8.4 "Cybersecurity event evaluation", 8.5 "Vulnerability analysis. The following could be used to evidence the processes used: ECE/TRANS/WP.29/2022/61 20 (b) Procedure for implementing cyber security incident response activities, including: (i) Field monitoring (obtaining information on incidents and vulnerabilities) (ii) Procedure for incident handling (iii) Procedures for discovering vulnerabilities (c) Demonstration of how the procedures are implemented.
7.2.2.5.	The vehicle manufacturer has demonstrated how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub- organizations in regards of the requirements of paragraph 7.2.2.2.	The intention of this requirement is to ensure that it can be shown that risks from suppliers are able to be known and can be managed within the processes described in the CSMS. The steps taken should be proportionate to the risks from what is supplied. The final implementation of the processes may be incorporated into bilateral agreement between the vehicle manufacturer and their suppliers. Within the CSMS there may be processes to: (a) identify risks associated with parts, components, systems or services provided by suppliers; (b) manage risks to the vehicle coming from service providers providing connectivity functions or services that a vehicle may rely on, this may include for example cloud providers, telecom providers, internet providers and authorised aftermarket service providers; (c) ensure contracted suppliers and/or service providers are able to evidence how they have managed risks associated with them. The processes may include consideration of validation or testing requirements that may be used to evidence that risks are appropriately managed; (d) delegate relevant requirements to relevant departments or sub-organisations of the manufacturer, in order to manage risks identified.	The following standards may be applicable: (e) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-06-10], [RQ-07-04], [RC-07-05]. The following could be used to evidence the processes used: (f) Contractual agreements in place or evidence of such agreements; (g) Evidenced arguments for how their processes will ensure suppliers / service providers will be considered in the risk assessment process; (h) Procedures/Methods of sharing information on risk between suppliers and manufacturers; (i) Existing solutions / contracts like ISMS (Information Security Management System) regulation can be used for evidence. This may be evidenced by certificates based on ISO/IEC 27001 or TISAX (Trusted Information Security Assessment eXchange).

		It is noted that it is possible to put requirements on Tier1 suppliers and to require they cascade it to Tier 2 suppliers. However, it may be difficult for a manufacturer to cascade requirements further down in the supply chain (especially legally binding requirements). The requirement should be considered unfulfilled if one of the following statements is true 1. Relevant contracts with suppliers and service providers do not have cyber security requirements. The requirement may be considered fulfilled if all the following statements are true 1. The vehicle manufacturer has a deep understanding of its supply chain, including sub-contractors and the wider risks it faces. The vehicle manufacturer considers factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs its risk assessment and procurement processes. 2. The vehicle manufacturer's approach to supply chain risk management considers the risks to its vehicle types arising from supply chain subversion by capable and well-resourced attackers. 3. The vehicle manufacturer has confidence that information shared with suppliers that is essential to the operation of your vehicle types is appropriately protected from sophisticated attacks. 4. The vehicle manufacturer can clearly express the security needs it places on suppliers in ways that are mutually understood and are laid in contracts. There is a clear and documented shared-responsibility model. 5. All network connections and data sharing with third parties is managed effectively and proportionately. 6. When appropriate, the vehicle manufacturer's incident management process and that of its suppliers provide mutual support in the resolution of incidents.	

Table 11 – Checklist for the CSMS audit

7. SPECIFIC CRITERIA FOR VEHICLE TYPE APPROVAL

7.1 INTERPRETATION OF REQUIREMENTS FOR THE TYPE APPROVAL

Table 12 describes the verification process for the requirements of UN Regulation No. 155 which are relevant for the approval of the vehicle type.

To each and every requirement a score will be assigned (2/1/0) during the assessment, as described in par. 3.3.2.

UN R155	Requirement	Interpretation with ref. to ECE/TRANS/WP.29/2022/61	Example of documents/proofs which may be provided (with ref. to ECE/TRANS/WP.29/2022/61)
7.3.1.	The manufacturer has a valid Certificate of Compliance* for the Cyber Security Management System relevant to the vehicle type being approved * For approvals prior to 1 July 2024, the manufacturer demostrates that vehicle type could not be developed in compliance with the CSMS and shows that cybersecurity was adequately considered during the development phase of the vehicle type concerned	The intention of this requirement is to ensure that there is a valid Certificate of Compliance for CSMS to enable type approval to be given for any new vehicle type and that it is appropriate to the vehicle type. For existing architectures that were developed before CSMS certification, it may not have been possible to develop the architecture in full compliance with that CSMS. Therefore, for type approvals before 1 July 2024, the provision for "adequate consideration" of cyber security applies but only to the development phase. The production and post production phases of those types must be in full compliance with the certified CSMS. Further technical modifications/updates leading to extensions of the existing type after 1 July 2024 should be performed as much as possible according to the processes defined in the CSMS for the development phase. Where there is deviation from the processes defined in the CSMS this should be explained and justified to the technical service or approval authority and the responsibility for the deviation assumed by the vehicle manufacturer at an appropriate management level. The following clarification should be noted: (a) "Relevant to the vehicle type being approved." means the CSMS should be applicable to the vehicle type being approved.	The following could be used to evidence the validity of the CSMS certificate: (b) The Certificate of Compliance for CSMS to demonstrate it is still valid; (c) Confirmation that the CSMS is appropriately applied to the vehicle type and any information required to provide assurance. (d) Information on how updates or extensions are managed within the CSMS for any update to type approvals before 1 July 2024."
7.3.2.	The vehicle manufacturer has identified and managed, for the vehicle type concerned, supplier-related risks	This requirement specifically references gaining sufficient information from the supply chain and is linked to 7.2.2.5. The intention of this requirement is to ensure that information presented (together with that from the manufacturer) is sufficient to allow an assessment to be conducted of the requirements 7.3.3. to 7.3.6. The following clarification should be noted: (a) "supplier-related risks" - The aim is that it can be shown that risks from suppliers are able to be known and can be managed. It is accepted that it is difficult to cascade requirements down in the supply chain beyond Tier 2 suppliers and ensure they are legally binding.	The following standards may be applicable: (b) ISO/SAE 21434. The following could be used to evidence the processes used: (c) Evidence in the form of contract sections with suppliers that deal with the requirements of this regulation.
7.3.3.	The vehicle manufacturer has identified, performed an exhaustive risk assessment and treated / managed the risks identified appropriately	The intention of this requirement is that the vehicle manufacturers shall identify the critical elements of a vehicle type with respect to cyber security and provide justification for how risks related to them are managed. The manufacturer should be able to provide justification for why they have identified elements of a vehicle type as critical (or not).	The following standards may be applicable: (g) ISO/SAE 21434 describes the way to define the concept. This also includes the consideration of critical elements based on risk treatment decisions. The results are documented in "[WP-09-03] Cybersecurity goals" and "[WP-09-06] Cybersecurity concept". It further describes exhaustive risk assessment in clause 15 "Threat analysis and risk assessment methods". This is documented in "[WP-09-02] TARA"; (h) ETSI TS 103 645 may be used for demonstrating the security of Internet of Things elements of a vehicle;

		The following clarifications should be noted (a) Critical elements may be elements contributing to vehicle safety, environment protection or theft protection. They could be parts which provide connectivity. They may also be parts of the vehicle architecture which are critical for sharing information or cyber security (e.g. gateways could be also considered critical); (b) The intention of this requirement is to ensure that risks shall be appropriately processed / managed by considering all threats including Annex 5, Part A and judging the necessity of countermeasures based on the results of risk analysis and risk evaluation; (c) The intention of this requirement is to allow the vehicle manufacturer to demonstrate the application of the relevant process in requirements 7.2.2.2. and 7.2.2.4. of the CSMS to the vehicle type; (d) The approval authority or technical service shall refer to Annex 5 of the Cyber Security Regulation to aid their assessment of the manufacturer's risk assessment; (e) The consideration of risks should consider the requirements of 7.3.4. and the requirement for proportionate mitigations; (f) The consideration of the threats and mitigations of Annex 5 within a risk assessment may lead to ratings like "not relevant" or "negligible risks".	(i) BSI PAS 1885 may be used. The following could be used to evidence this requirement: (j) The vehicle type claimed; (k) An explanation of why elements within the vehicle type are critical; (l) What security measures are implemented, including information on how they work; (m) Information on any security measures should permit the Technical Service/ Approval Authority to both be assured that they do what the manufacturer intends and that vehicles in production will use the same measure as presented to the Approval Authority/Technical Service for the vehicle type. Confidentiality of specifics and how these are handled should be agreed and recorded.
7.3.4.	The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment	The intention of this requirement is to ensure that vehicle manufacturers implement appropriate mitigation measures in accordance with the results of their risk assessment. The manufacturer should provide reasoned arguments and evidence for the mitigations they have implemented in the design of the vehicle type and why they are sufficient. This may include any assumptions made, for example about external systems that interact with the vehicle. The technical mitigations from Annex 5, Parts B and C shall be considered wherever applicable to the risks to be mitigated. The Manufacturer may present a rationale not only for a listed mitigation from Annex 5 being "not relevant or not sufficient", but also may present a rationale, that another mitigation other than the ones listed in Annex 5 is appropriate to the respective risk. That rationale may be substantiated by a risk assessment and risk rating showing the appropriateness of the alternative mitigation. This is to allow the adoption of new or improved defensive technologies. For existing architectures that were developed before the enforcement of UN Regulation No. 155, it may not have been possible to develop the architecture so that all mitigations in Annex 5, part B and C were implemented. Therefore, for approvals first issued before 1 July 2024,	The following standards may be applicable: (d) ISO/SAE 21434 describes the determination of risk and the deduced Cybersecurity goals and concept based on the identified risks. The results are documented in "[WP-09-03] Cybersecurity goals" and "[WP-09-06] Cybersecurity concept"; (e) BSI PAS 11281: 2018 and other standards regarding claims, arguments and evidence may be used to justify the design decisions of the manufacturer. The following could be used to evidence the mitigations used: (f) Evidence that mitigation measures were introduced according to the necessity of measures, this includes: (i) the reason, if mitigation measures other than Annex 5 Part B and C are applied; (ii) the reason, if mitigations listed in Annex 5 are not applied; (iii) the reason, if mitigation measures are determined to be unnecessary.

		other appropriate mitigations for identified cyber security risks are permitted. Further technical modifications/updates leading to extensions of those existing types after 1 July 2024 should be performed as much as possible in accordance with Annex 5. This should consider the risks and confirm they continue to be managed or reduced. Where there is deviation from Annex 5 this should be explained and rationalised. The following clarifications should be noted: (a) The design decisions of the manufacturer should be linked to the risk assessment and risk management strategy. The manufacturer should be able to justify the strategy implemented; (b) The term "proportionate" should be considered when choosing whether to implement a mitigation and what mitigation should be implemented. If the risk is negligible then it may be argued that a mitigation would not be necessary; (c) Protection from identified risks means to mitigate the risk.	
7.3.5.	The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data	The following clarifications should be noted: (a) "appropriate and proportionate measures" requires that the manufacturer is able to justify how risks associated with any dedicated environment, as defined in their risk assessment, are managed; (b) Dedicated environments can be on the vehicle. If the vehicle interacts with servers or services located off the vehicle (for example in the cloud) then the risks to the vehicle originating from them, with respect to their cyber security, should be considered.	The following standards may be applicable: (c) ISO/SAE 21434 describes steps to make conclusions for the architecture. "[WP-15-03] Threat scenarios" documents the potential threats to the storage and execution of aftermarket software, services, application or data. In "[WP-09-06] Cybersecurity concept" the appropriate and proportionate measures are being described. The following could be used to evidence this requirement: (d) A description of the dedicated environment; (e) What security measures are implemented, including information on how they work; (f) Information on any security measures should permit the Approval Authority/Technical Service to both be assured that they do what the manufacturer intends and that vehicles in production will use the same measure as presented to the Approval Authority/Technical Service for the vehicle type. Confidentiality of specifics and how these are handled should be agreed and recorded; (g) Annex 5 of the cyber security Regulation shall be referred to.
7.3.6.	The vehicle manufacturer shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented	The test results should be valid at time of type approval. The Technical Service may perform security tests to confirm the results. The following clarifications should be noted: (a) The aim of any security measures will be to reduce the risks. Testing should support justification for the security measures implemented.	The following standards may be applicable: (b) Manufacturers may describe the verification and validation measure implemented in accordance with ISO/SAE 21434 in form of "[WP-10-07] Integration and verification report", "[WP-11-01] Validation report". The following could be used to evidence this requirement: (c) What is tested and why (e.g. what measures of success for the test look like); (d) Methodology used and why (e.g. this may include notes on the extent and effort contained within the testing); (e) Who has performed the tests and why (e.g. in-house, a supplier or an external organization and any relevant information regarding their qualification/experience); (f) Confirmation of its successful outcome (this may include the pass/fail criteria and result of the test).

7.3.7.	The vehicle manufacturer, for the vehicle type shall: (a) Detect and prevent cyber-attacks; (b) Support the monitoring capability; (c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks	The intention of this requirement is to ensure that there are specific measures implemented for the vehicle type to monitor for changes in the threat landscape, detect and prevent cyber-attacks and have the capability to forensically support the analysis of any attempted or successful attack. The following clarifications should be noted: (a) Measures with regard to this clause may be implemented on the vehicle type or in its operational environment, e.g. the backend, the mobile network "for the vehicle type"; (b) Measures should primarily look to prevent cyber-attacks being successful, with reference to 7.3.4. and 7.3.5. to protect against risks identified in the risk assessment; (c) Measures to prevent cyber-attacks being successful against all vehicles of a vehicle type may additionally be delivered asynchronously, i.e. after the actual event of a cyber-attack and its analysis; (d) Data forensic capability may include the ability to provide and analyse log data, diagnostic error codes, vehicle operational information, backend information to investigate cyber-attacks; (e) Data forensic capability may include a circular buffer of persisting log data that supports investigatory procedures. It is noted that paragraph 1.3., and compliancy with data privacy laws, are particularly relevant to this requirement.	The following standards may be applicable: (f) ISO/SAE 21434. Identifying sources for cybersecurity monitoring is provided in [RQ-08-01] and documented in "[WP-08-01] Sources for cybersecurity information". The results of analysis and how to document it is described in "[WP-08-05] Vulnerability analysis". The following could be used to evidence this requirement: (g) Attack prevention measures applied to the vehicle type; (h) Demonstration of how a vehicle type's preventive measures and monitoring activities perform; (i) Demonstration of how forensic analysis is performed.
7.3.8.	Cryptographic modules used for the purpose of this Regulation shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use	The following clarifications should be noted: A consensus standard may be an internationally recognised standard, or it may be a national standard that is commonly used, e.g. FIPS. The intent of this requirement is to ensure encryption methods used can be justified.	Where encryption measures are implemented, based on the results of risk analysis and risk assessment, the manufacturer should be able to: (a) Explain whether the encryption algorithm or measure complies with a current consensus standard; and (b) Explain the reason for the choice of encryption and why it adequately mitigates the risk identified.

Table 12 – Checklist for the type approval

7.2 TECHNICAL ASSESSMENT AND TESTING

During the assessment for the approval of the vehicle type, the Technical Service will collect all useful elements for the establishing a plan for the repetition of a certain number of physical tests on the vehicle representative of the vehicle type in order to check the effectiveness of the mitigation measures adopted by the manufacturer to counteract the identified threats.

The Technical Service will decide which physical tests shall be repeated under its own supervision at the manufacturer's site or at an accredited laboratory and will evaluate the outcome by drafting a specific test report.

The decision on which physical tests need to be repeated will be based on the assessment of the risk analysis and on the results of testing already performed either by the manufacturer or by accredited laboratories during the vehicle type development phase. The Technical Service will pay particular attention to the list of hazards, threats and mitigation measures given in Annex 5 to UN Regulation No. 155.

ANNEX 1

EXAMPLE OF COMPLIANCE MATRIX STRUCTURE
[Par. 7.2.2.2.(b) and 7.2.2.2.(c) of UN R155]

Example

7.2.2.2. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include: (b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered;	The aim of this requirement is for a manufacturer to demonstrate the processes and procedures they use to identify risks to vehicle types. Processes implemented should consider all probable sources of risk. This shall include risks identified Annex 5 of the Cyber Security Regulation e.g. risks arising from connected services or dependencies external to the vehicle. Sources for risk identification may be stated. These may include: (a) Vulnerability/ Threats sharing platforms; (b) Lessons learned regarding risks and vulnerabilities.	This requirement is covered by the processes described in: • §8-Risk assessment methodology overview • §10-Threat Analysis and Risk Assessment (TARA) • §11-Risk treatment
7.2.2.2. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include: (c) The processes used for the assessment, categorization and treatment of the risks identified;	The aim of this requirement is that the manufacturer demonstrates the processes and rules they use to assess, categorize and treat risks identified.	This requirement is covered by the processes described in: • §8-Risk assessment methodology overview • §10-Threat Analysis and Risk Assessment (TARA) • §11-Risk treatment

ANNEX 2

TEMPLATE OF APPLICATION FOR CSMS AUDIT AND CERTIFICATION
[Par. 6.2. of UN R155]

(°)

Al Ministero delle Infrastrutture
e della Mobilità Sostenibili
Dipartimento per la mobilità sostenibile
Direzione Generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione
Divisione 3

Oggetto: Richiesta di verifica del sistema di gestione della sicurezza informatica (CSMS) ai fini del rilascio della certificazione ai sensi del Regolamento UN R155
Subject: Request for Cybersecurity Management System (CSMS) assessment aimed at certification issue in compliance with UN Regulation No. 155

Il sottoscritto / *The undersigned* ____________________

In qualità di / *In my capacity of* ____________________ (*)

del Costruttore / *of the OEM* ____________________

con sede in / *based in* ____________________

email / *email* ____________________

rivolge istanza affinché per lo/gli stabilimento/i sito/i in
makes an application in order to, for the plant/plants based in ____________________

a) sia verificata l’idoneità del CSMS / *assess the CSMS compliance* □

b) sia confermata l’idoneità del CSMS / *confirm the CSMS compliance* □

A tal fine dichiara che il Costruttore presso il suindicato stabilimento produce:
For this purpose I declare that the OEM at the above mentioned plant/plants manufactures:

□ Veicoli / *Vehicles* ____________________ (**)

Al riguardo allega alla presente richiesta i seguenti documenti (+):
To this extent the following documents are attached to the application (+):

- Attestazione dei versamenti previsti: CCP 9001 di euro 10,20 e CCP 4028 di euro 32.00;
  Receipt of the requested payments
- Estremi della Camera di commercio o documento equivalente per Stati esteri;
  References of the Chamber of Commerce or equivalent document for foreign Countries
- Descrizione sintetica della produzione svolta nel sito per il quale si chiede l'ispezione;
  General description of the current operations for the plant/plants covered by the application
- Descrizione del sistema di gestione della sicurezza informatica per il sito per il quale si chiede l'ispezione;
  Description of cyber security management system for the plant/plants covered by the application
- Certificazioni ISO e/o di altri Stati membri ove presenti;
  ISO certificates and/or certificates granted by other Type Approval Authorities, if existing
- Copia della domanda di omologazione presentata (nel caso di avvio della produzione);
  Copy of the type approval application (in the case of start of production)
- Accordo nel caso di produzione presso un sito di altro Costruttore.
  Signed agreement in the case of production taking place at another OEM's plant

Si resta in attesa delle decisioni da parte della Commissione per la valutazione del CSMS di codesto ufficio.
Waiting for the decisions taken by the Commission being charged of the CSMS audit

Luogo, data
Place, date ______________________

Firma (***)
Signature

____

Note:
Notes:

(°) Costruttore: utilizzare carta intestata della ditta
OEM: use the letterhead of the Manufacturer

(*) titolare, amministratore delegato, rappresentante legale, mandatario o persona legalmente autorizzata o delegata alla firma delle istanze e alla effettuazione di dichiarazioni vincolanti per il Costruttore.
owner, CEO, legal representative, emissary or person legally authorised or designated to sign the application and to make declarations that are binding for the OEM

(**) indicare la tipologia dei veicoli, dei dispositivi prodotti e la relativa categoria internazionale o nazionale (es. autovetture, autocarri, autobus, trattori. ecc.).
specify the type of vehicles and the relevant International or National category (e.g. passenger cars, commercial vehicles, buses, tractors, etc…)

(***) timbro della ditta, nome e qualifica del firmatario. Allegare documento di riconoscimento del firmatario.
seal of the manufacturer, name and position of the undersigned (ID card of the undersigned is attached)

(+) documentazione obbligatoria.
mandatory documentation

Istruzioni per la compilazione: riportare le informazioni nei campi grigi
Instructions: provide the requested information by filling-in the grey fields

ANNEX 3

TEMPLATE OF APPLICATION FOR A VEHICLE TYPE APPROVAL

[Par. 3.1. of UN R155]

Al Ministero delle infrastrutture e della mobilità sostenibili

Dipartimento per la mobilità sostenibile

Direzione Generale …

Servizio Tecnico (esplicitare) …

Il sottoscritto / *The undersigned*
……………………………………………………………………………..……….……………
…………………………………

in qualità di **(1)**:
in my capacity of ***(1):***

□ legale rappresentante / *legal representative*

□ rappresentante accreditato presso il Centro Prova Autoveicoli di / *representative accredited to the Technical Service of* …….………………………………………………….

□ mandatario (se ricorre) / *emissary (if applicable)*
………...……………………………………………………………………………………..

del costruttore / *of the OEM*
……………………………………………………………………………………………….

con sede legale in / *with registered office in*
………...………………………………………………………………………………………
e sito produttivo / *and manufacturing plant*…………………..……………………………………..

rivolge istanza affinché il veicolo (categoria)
makes an application so that the following vehicle (category)
....)
(2)(3):

Marca (denominazione commerciale) / *Make (brand name)*.. **(4)**

nel tipo di seguito indicato, possa ottenere, ai sensi della seguente normativa **(5)**:
of the following type be granted, with reference to the following regulation ***(5):***

........…………………………………………………………………………………………

L'OMOLOGAZIONE / ESTENSIONE / AGGIORNAMENTO / REVISIONE DELL'OMOLOGAZIONE **(6)**:
*THE TYPE APPROVAL / AN EXTENSION / AN UPDATE / A REVISION OF THE TYPE APPROVAL **(6)**:*

TIPO **(7)** *TYPE **(7)***	N° MARCHE OPERATIVE **(8)** *N° OF TAX STAMP **(8)***	DATA VERSAMENTO *DATE OF DEPOSIT*	CODICE TARIFFA **(9)** *TARIFF CODE **(9)***
……………..	………………………………	……………………	…………………..…..

DICHIARAZIONI
DECLARATIONS

Si dichiara che per la stessa omologazione:
I hereby declare that for the same approval:

a) non è stata presentata analoga domanda presso un altro Stato membro/altro Paese contraente dell'Accordo internazionale di Ginevra **(10)** o presso altro Centro Prova Autoveicoli;
no other application was made to a different Member State/Contracting Party of the '58 Agreement ***(10)*** *or to another Technical Service*

b) nessuna autorità di omologazione ha rifiutato di rilasciare un'omologazione del tipo in questione;
no other Type Approval Authority has refused to grant the approval for the relevant type

c) nessuna autorità di omologazione ha revocato l'omologazione del tipo in questione;
no other Type Approval Authority has withdrawn the approval for the relevant type

d) non è stata revocata la domanda di omologazione per il tipo in questione.
the application for approval of the relevant type has not been rejected

La documentazione tecnica prevista (scheda informativa ed elaborati tecnici) è allegata e/o verrà perfezionata nell'ambito delle verifiche e prove. **(11)**
The requested technical documentation (communication file and technical papers) is attached and/or will be produced during the relevant assessment and testing ***(11)***

Sono stati assolti i previsti oneri stabiliti dalla normativa vigente secondo la voce tariffaria ~~6~~ della tabella 3 della legge 01/12/1986 n. 870 con pagamento tramite PagoPA secondo il tariffario individuabile al seguente link
Duties specified by the legislation in force have been fulfilled in compliance with the tariff code 6 under table 3 of Law 01/12/1986 n. 870 through a deposit with PagoPA following the price list available at the following link
https://www.ilportaledellautomobilista.it/web/portale-automobilista/pagamenti-pagopa.

Si fa presente che i prototipi necessari per le verifiche e prove sono già disponibili/sono disponibili
The prototypes needed for the relevant assessment and testing are already available/will be available

Dal / *from* ……………..**(12).**

Le verifiche e prove si svolgeranno presso il sito produttivo/laboratorio
Assessment and testing will be performed at the following plant/laboratory
…………………………………………………………………….**(13)**

Data e Luogo
Date and Place

……………………………..

………………….

Firma del richiedente **(14)**
Signature of the applicant ***(14)***

……………………………

Note:
Notes:

(1) Contrassegnare la voce che ricorre
Tick as applicable

(2) Depennare i casi che non ricorrono
Strikeout the items which do not apply

(3) Per i veicoli e i sistemi indicare la categoria secondo quanto previsto dal Codice della Strada dagli artt. 52-60 e/o dal regolamento UE/UNECE, ove ricorre
For vehicles and systems specify the category as specified by the Road Traffic Law (articles 52 to 60) and/or by the EU/UNECE regulation, if applicable

(4) Se ricorre indicare la marca del prodotto
If applicable specify the brand name

(5) Indicare la norma che si intende applicare (Regolamento UNECE, Regolamento UE, Norma nazionale, altro):
Specify the applicable regulation (UN Regulation, EU Regulation, National Standard, other)

a) Per il Regolamento UNECE, indicare il numero del Regolamento, l'emendamento e il supplemento
In case of a UN Regulation, specify the number, series of amendments and supplement

b) Per il regolamento UE, indicare il Regolamento base e l'ultimo regolamento di modifica (se esistente)
In case of a EU Regulation, specify the base Regulation and the latest amendment available (if existing)

c) Per la normativa nazionale, indicare l'articolo del Codice/Regolamento o il DM pertinente con anche, se prevista, la norma CUNA/ISO di riferimento
In case of a National Standard, specify the Law/Regulation article or the relevant Decree together with the reference CUNA/ISO standard if applicable

(6) Depennare i casi che non ricorrono. In caso di estensione/aggiornamento/revisione completare con gli estremi di omologazione
Strikeout the items which do not apply. In case of extension/update/revision also provide the type approval details

(7) Ove ricorrano varianti e versioni, allegare una tabella nella quale siano specificate le differenze che determinano l'introduzione di varianti/versioni ai fini tariffari
Where variants and versions are foreseen, provide (for tariff purposes) a table to highlight the differences which demand for the introduction of such variants/versions

(8) Da completare a cura del Centro Prova Autoveicoli
To be completed by the Technical Service

(9) Indicare uno o più dei codici previsti dalla tabella 3 legge 870/86
List one or more codes as foreseen by table 3 of Law 870/86

(10) Depennare i casi che non ricorrono
Strikeout the items which do not apply

(11) Inserire elenco allegati
Enter the list of attachments

(12) Barrare la voce che non ricorre e indicare, se ricorre, la data di disponibilità
Strikeout the item that does not apply and specify the availability date, if applicable

(13) Da completare con la denominazione, se esistente, del laboratorio (la denominazione/indicazione con la sede è obbligatoria se trattasi di Ente terzo). Indicare in ogni caso se il laboratorio è/non è certificato ISO 17025 e fornire, in caso positivo, gli estremi di certificazione ISO 17025 n° ……..
To be completed with the name of the laboratory, if applicable (the name and address is requested in case of a third party lab). Specify in any case if the laboratory is/is not ISO 17025 accredited and, in the affirmative, provide the accreditation number n°…….

(14) Indicare in stampatello per esteso nome, cognome e qualifica di chi firma (come designato dal costruttore e depositato presso il CPA) ovvero – in caso di mandatario - far seguire con le parole "per conto di"
Specify in block letters and in full the first name, family name and position of the applicant (as identified by the OEM and registered at the Technical Service) or, in the case of an emissary, complete with the words "on behalf of"

ANNEX 4

MODEL OF REPORT FOR CSMS AUDITING

Ministero delle Infrastrutture e della Mobilità Sostenibili

Dipartimento per la mobilità sostenibile

Direzione generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione
Divisione 3

VERBALE n° *AUDIT N.*	DEL *DATE*

Conformità al Sistema di Gestione della Cybersicurezza (CSMS)
Compliance with the Cyber Security Management System (CSMS)

Verifica delle specifiche del costruttore al Punto 7. del Regolamento ECE N. 155
Verification of the manufacturer's specifications at Point 7. of ECE Regulation No. 155

COSTRUTTORE / *MANUFACTURER*

Denominazione ______________________

Name ______________________

Sede legale ______________________

Registered Office ______________________

Mandatario in Italia ______________________

Mandatary in Italy ______________________

Stabilimenti di produzione ______________________

Production plant(s) ______________________

____

____

Categorie di veicoli per le quali il Costruttore richiede Audit triennale di processo
Vehicle categories for which the manufacturer requires triennial process Audits

□ M ______________________

□ N ____________________

PREMESSA / *PREMISE*

Il costruttore dichiara di aver adottato tutte le misure necessarie a ottemperare agli obblighi sul sistema di gestione della cybersicurezza (CSMS).
The manufacturer declares that it has taken all necessary measures to comply with the requirements for the cybersecurity management system (CSMS).

Sì / Yes □ **No** □

FIRMA DEI FUNZIONARI / *SIGNATURE OF OFFICIALS*

1 CARATTERISTICHE GENERALI DELL'ORGANIZZAZIONE PRODUTTIVA *GENERAL CHARACTERISTICS OF THE PRODUCTIVE ORGANIZATION*

1.1 Il Costruttore ha predisposto un'organizzazione aziendale, responsabilità e ambiti di competenza del personale addetto, risorse e misure opportune, piani di controllo documentati, istruzioni per l'esecuzione dei test, gestione dei report, verifica dei risultati e controllo del piano per verificare che il sistema di gestione della cybersicurezza (CSMS) sia conforme al regolamento.

The Manufacturer has in place a business organization, responsibilities and areas of responsibility of relevant personnel, appropriate resources and measures, documented control plans, test execution instructions, report management, results verification, and plan control to verify that the cybersecurity management system (CSMS) is in compliance with the regulation.

2 □ **1** □ **0** □

DATA DELLA PRECEDENTE CERTIFICAZIONE
PREVIOUS CERTIFICATION DATE ________

N.ro DELLA PRECEDENTE CERTIFICAZIONE
PREVIOUS CERTIFICATION N. ________

0 = assenza totale del requisito / *total absence of the requirement*
1 = soddisfacimento parziale (necessarie azioni di miglioramento) / *partial satisfaction (necessary improvement actions)*
2 = soddisfacimento totale / *total satisfaction*

2 Verifica preliminare del Sistema di Gestione della Cybersicurezza (CSMS) *Preliminary verification of the Cybersecurity Management System (CSMS)*

7.1 - Reg. ECE N. 155

7.1.1 Il costruttore del veicolo dispone di processi che verificano che le prescrizioni del presente regolamento non limitano le disposizioni o le prescrizioni di altri regolamenti ONU.

2 □ **1** □ **0** □

The vehicle manufacturer has processes that verify that the requirements of this Regulation shall not restrict provisions or requirements of other UN regulations.

FIRMA DEI FUNZIONARI / *SIGNATURE OF OFFICIALS*

3 Controllo della conformità del Sistema di Gestione della Cybersicurezza (CSMS)
Cybersecurity Management System (CSMS) Compliance Monitoring

7.2 del Regolamento ECE N. 155

7.2.2.1.	Il costruttore del veicolo dispone di un sistema di gestione della cybersicurezza che si applica alle seguenti fasi: (a) fase di sviluppo, (b) fase di produzione, (c) fase di post-produzione. *The vehicle manufacturer has a Cyber Security Management System which applies to the following phases: (a) development phase, (b) production phase, (c) post-production phase.*	2	1	0
7.2.2.2.(a)	Il costruttore dispone di processi all'interno della propria organizzazione per gestire la cybersicurezza. *The vehicle manufacturer has processes used within the manufacturer’s organization to manage cyber security.*	2	1	0
7.2.2.2.(b)	Il costruttore dispone di processi utilizzati per l’identificazione dei rischi per i tipi di veicolo; nell’ambito di tali processi prende in considerazione le minacce di cui all'Allegato 5, Parte A del Regolamento e altre minacce pertinenti. *The vehicle manufacturer has processes used for the identification of risks to vehicle types; within these processes, the threats in Annex 5, Part A of the Regulation and other relevant threats are considered.*	2	1	0
7.2.2.2.(c)	Il costruttore dispone di processi utilizzati per la valutazione, la categorizzazione e il trattamento dei rischi individuati. *The vehicle manufacturer has processes used for the assessment, categorization and treatment of the risks identified.*	2	1	0
7.2.2.2.(d)	Il costruttore dispone di processi per verificare che i rischi individuati siano gestiti in modo adeguato. *The vehicle manufacturer has processes in place to verify that the risks identified are appropriately managed.*	2	1	0
7.2.2.2.(e)	Il costruttore dispone di processi utilizzati per testare la cybersicurezza di un tipo di veicolo. *The vehicle manufacturer has processes used for testing the cyber security of a vehicle type.*	2	1	0
7.2.2.2.(f)	Il costruttore dispone di processi utilizzati per garantire che la valutazione del rischio sia mantenuta aggiornata. *The vehicle manufacturer has processes used for ensuring that the risk assessment is kept current.*	2	1	0
7.2.2.2.(g)	Il costruttore dispone di processi utilizzati per monitorare, individuare e rispondere agli attacchi e minacce informatiche e alle vulnerabilità dei tipi di veicolo e di processi	2	1	0

	utilizzati per valutare se le misure di cybersicurezza attuate siano ancora efficaci alla luce delle nuove minacce informatiche e vulnerabilità individuate. *The vehicle manufacturer has processes used to monitor for, detect and respond to cyberattacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.*	
7.2.2.2.(h)	Il costruttore dispone di processi utilizzati per fornire dati pertinenti a sostegno dell'analisi di attacchi informatici tentati o riusciti. *The vehicle manufacturer has processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.*	**2** **1** **0**
7.2.2.3.	Il costruttore dispone di processi utilizzati nel suo sistema di gestione della cybersicurezza che, sulla base della categorizzazione riferite ai commI (c) e (g) del punto 7.2.2.2, garantiranno che le minacce informatiche e le vulnerabilità siano attenuate entro un lasso di tempo ragionevole. *The vehicle manufacturer has processes used within their Cyber Security Management System that ensure that, based on categorization referred to paragraphs 7.2.2.2.(c) and 7.2.2.2.(g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.*	**2** **1** **0**
7.2.2.4.	Il costruttore dispone di processi utilizzati all'interno del proprio sistema di gestione della cybersicurezza che garantiscono che il monitoraggio riferito al comma (g) del punto 7.2.2.2. sia continuo, includa i veicoli dopo la prima immatricolazione e sia capace di analizzare e rilevare minacce informatiche, vulnerabilità e attacchi attraverso i dati e i log dei veicoli. *The vehicle manufacturer has processes used within their Cyber Security Management System that ensure that the monitoring referred to in paragraph 7.2.2.2 (g) shall be continual, include vehicles after first registration and is capable to analyse and detect cyber threats, vulnerabilities and cyberattacks from vehicle data and vehicle logs.*	**2** **1** **0**
7.2.2.5.	Il costruttore ha dimostrato in che modo il suo sistema di gestione della cybersicurezza gestirà le eventuali dipendenze con fornitori, fornitori di servizi o sub-organizzazioni del costruttore per quanto riguarda le prescrizioni riferite al punto 7.2.2.2.. *The vehicle manufacturer has demonstrated how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub- organizations in regards of the requirements of paragraph 7.2.2.2.*	**2** **1** **0**

FIRMA DEI FUNZIONARI / *SIGNATURE OF OFFICIALS*

NUMERO DI RISPOSTE / *NUMBER OF RESPONSES*	
NUMERO DI "ZERO" (N) / *NUMBER OF "ZERO" (N)*	
SE I TEST SONO STATI EFFETTUATI DA SOCIETA' ESTERNA AL COSTRUTTORE SI ATTRIBUISCE UN PUNTO ADDIZIONALE / *IF THE TESTS WERE CARRIED OUT BY COMPANY OUTSIDE THE MANUFACTURER AN ADDITIONAL POINT IS AWARDED*	

TOTALE PUNTEGGIO / *TOTAL SCORE*	

MEDIA OTTENUTA (M) / *AVERAGE OBTAINED (M)* TOTALE PUNTEGGIO ÷ NUMERO DI RISPOSTE / *TOTAL SCORE ÷ NUMBER OF ANSWERS*	

Il numero di risposte è riferito a quelle applicabili al costruttore e viene utilizzato per il calcolo del punteggio finale

The number of responses refers to those applicable to the constructor and is used to calculate the final score

OSSERVAZIONI / *OBSERVATIONS*

FIRMA DEI FUNZIONARI / *SIGNATURE OF OFFICIALS*

NOTA / *NOTE*

Le valutazioni si basano su tre livelli: / *Evaluations are based on three level* :

2 – esiste ed è operante; / *it exists and is operational*;
1 – esiste ma incompleto/non documentato ma operante/operante saltuariamente; /*t exists but incomplete/undocumented but operating/operating occasionally*;
0 – non esiste/inoperante. / *does not exist/operates*.

A conclusione della stesura del presente verbale di verifica la valutazione finale del Costruttore sarà:

At the conclusion of the preparation of this Verification Report, the OEM's final evaluation will be:

DI IDONEITA' se sono verificate entrambe le condizioni seguenti: / ***ELIGIBLE*** *if both of the following conditions are met*:

- assenza di "ZERO": / *absence of "ZERO":* **N=0**
- media M ottenuta: */ average M obtained*: **1,7 ≤ M**

DI IDONEITA' CON RISERVA se sono verificate entrambe le condizioni seguenti: / ***ELIGIBLE WITH RESERVATION*** *if both of the following conditions are met*:

- assenza di "ZERO": / *absence of "ZERO":* **N=0**
- media M ottenuta: */ average M obtained*: **1,4 ≤ M < 1,7**

DI NON IDONEITA' se si verifica anche solo una delle seguenti condizioni: / ***NOT ELIGIBLE*** *if only one of the following condition is met*:

- numero di "ZERO": / *number of "ZERO":* **N > 0**
- media M ottenuta: / *average M obtained*: **M < 1,4**

VALUTAZIONE FINALE / *FINAL EVALUATION*

In esito a quanto riportato sul presente verbale,
According to the final evaluation reported in this audit,

SI RITIENE / *IS CONSIDERED*

che il costruttore indicato in epigrafe, presso i locali soggetti a sopralluogo ha illustrato le proprie misure del sistema di gestione della cybersicurezza (CSMS) in conformità al regolamento ECE N. 155 con valutazione finale:
that the manufacturer named in the epigraph, at the premises subject to inspection, has illustrated its cybersecurity management system (CSMS) measures in accordance with ECE Regulation No. 155 with the final evaluation:

IDONEA
ELIGIBLE □

IDONEA CON RISERVA
ELIGIBLE WITH RESERVATION □

NON IDONEA
NOT ELIGIBLE □

e si trasmette il presente verbale per le determinazioni conseguenti.
and this audit is transmitted for the consequent determinations.

Luogo e data del sopralluogo / *Place and date of inspection*

____

FIRMA DEI FUNZIONARI / *SIGNATURE OF OFFICIALS*

Nome	Cognome	Ufficio di appartenenza
Name	*Surname*	*Office of affiliation*
____________________	____________________	D.G. MOT. - DIV. 3
____________________	____________________	D.G. MOT. - DIV. 3

ANNEX 5

MODEL OF REPORT FOR VEHICLE TYPE ASSESSMENT AND TESTING

Ministero delle Infrastrutture e della Mobilità Sostenibili

Dipartimento per la mobilità sostenibile

Direzione Generale …………

Servizio Tecnico (esplicitare) …

-

Rapporto di prova n° ___________-

Test report no.

Relativo alle verifiche e prove per l'omologazione dei veicoli per quanto concerne la cyber sicurezza e al sistema di gestione della cyber sicurezza - Regolamento UNECE N. 155.

Related to checks and tests for EEC type approvals with regard regards to cyber security and cyber-security management system- UNECE Regulation No. 155

Marca: *Make:*	XXXX op./or XXXX
Tipo e denominazione commerciale del veicolo: *Type and trade name of manufacturer:*	XXXXXXXXXXX
Veicoli appartenenti allo stesso tipo ai sensi del punto 2.1.: *Vehicles belonging to the same type under of point 2.1.:*	Vedere schemi n° XXXX *see scheme no….*
Categoria del veicolo: *Category of the vehicle:*	XX

Nome e indirizzo del costruttore: *Name and address of manufacturer:*	XXXXXXXXXXX
Caratteristiche del veicolo: *Vehicle characteristics:*	vedere scheda informativa /*see information document* XXXXXXXX
Data della domanda: *Application request date:*	00/00/0000
Luogo e data delle verifiche e prove: *Place and date of checks and tests:*	Torino, 00/00/0000
Nome e indirizzo del laboratorio di prove: *Name and address of the test laboratory:*	--

PREMESSA / *INTRODUCTON*

- L’atto normativo di cui all’oggetto, prevede un modello di verbale di prova: **NO**

  *A standard test report was provided in the regulatory act mentioned in the subject: **NO***

PROVE / *TEST*

- Il costruttore e l’autorità di omologazione o il servizio tecnico hanno identificato una configurazione peggiore da sottoporre a prova rappresentativa di tutte le configurazioni? **SI/NO/N.A.**
  *The manufacturer and the type-approval authority or technical service have identified a worst-case configuration, to test that configuration as representatives of all the configurations? **YES/NO/N.A.***

- Informazioni relative al modo in cui è stata trovata la configurazione peggiore del sistema, del componente o dell’entità tecnica indipendente: **SI/NO/N.A.**
  *Information about how the worst-case system, component or independent technical unit configuration was found: **YES/NO/N.A.***

- Sono stati utilizzati metodi di prova diversi da quelli prescritti negli atti normativi applicabili e da essi consentiti? **SI/NO/N.A.**
  *Other test methods than those prescribed in the applicable regulatory acts and by them permitted had been used? **YES/NO/N.A.***

- Descrizione dei metodi utilizzati e consentiti diversi da quelli prescritti negli atti normativi applicabili: **SI/NO/N.A.**
  *Description of test methods used and different than those prescribed in the applicable regulatory acts: **YES/NO/N.A.***

- Campionamento: **SI/NO/N.A.**
  *Sampling**: YES/NO/N.A.***

a) identificazione dei veicoli, del sistema, del componente o dell’entità tecnica indipendente sottoposto/a a prova: **SI/NO/N.A.**

*identification of the vehicle, system, component or separate technical unit tested: **YES/NO/N.A.***

b) descrizione dettagliata delle caratteristiche del veicolo, del sistema, del componente o dell’entità tecnica indipendente prescritte dall’atto normativo applicabile di cui all’allegato II del regolamento (UE) 2018/858:

detailed description of the vehicle, system, component or separate technical unit characteristics required by the applicable regulatory act listed in Annex II to Regulation (EU) 2018/858:

- vedere scheda informativa n. XXXXXXXX.

- see information document no. XXXXXXXX.

c) risultati delle verifiche prescritte stabiliti dall’atto normativo applicabile: vedi tabella successiva ed allegati

results of the prescribed checks required by the applicable regulatory act: see next table and annex

Sul veicolo/prototipo presentato alle prove sono stati condotti i seguenti accertamenti:

On the prototype vehicle under examination, have been verified as listed below:

7.3	Prescrizioni per i tipi di veicolo / _Requirements for vehicle types_		
7.3.1	Il costruttore è in possesso di un certificato di conformità valido* per il sistema di gestione della cibersicurezza relativo al tipo di veicolo da omologare. *Per le omologazioni anteriori al 10 luglio 2024, Il costruttore dimostra che il veicolo non è stato sviluppato in maniera conforme al CSMS, e dimostra che la cibersicurezza è stata presa in considerazione durante la fase di sviluppo del tipo di veicolo in questione. _The manufacturer have a valid Certificate of Compliance* for the Cyber Security Management System relevant to the vehicle type being approved._ _* For approvals prior to 1 July 2024, the manufacturer demostrate that vehicle type could not be developed in compliance with the CSMS and shows that cybersecurity was adequately considered during the development phase of the vehicle type concerned._		□2 □1 □0 - vedi Certificato di conformità per il CSMS allegato* - see c_ertificate of Compliance for the CSMS annex*_ *Vedi allegato XXYY per le omologazioni anteriori al 10 luglio 2024 _*See annex XXYY for approvals prior to 1 July 2024_
7.3.2	Il costruttore del veicolo ha individuato e gestito, per il tipo di veicolo da omologare, i rischi connessi ai fornitori. _The vehicle manufacturer has identified and managed, for the vehicle type concerned, supplier-related risks._		□2 □1 □0 Vedi allegato XXYY _See annex XXYY_
7.3.3	Il costruttore del veicolo ha individuato, valutato e trattato/gestito i rischi individuati, in maniera adeguata. _The vehicle manufacturer has identified, performed an exhaustive risk assessment and treated / managed the risks identified appropriately._		□2 □1 □0 Vedi allegato XXYY (rif. allegato 5, parte A) _See annex XXYY (ref. Annex 5, Part A)_
7.3.4	Il costruttore del veicolo ha protetto il tipo di veicolo dai rischi individuati nella sua valutazione del rischio. _The vehicle manufacturer has protected the vehicle type against risks identified in the vehicle manufacturer's risk assessment._		□2 □1 □0 Vedi allegato XXYY (rif.allegato 5, parte B-C) _See annex XXYY (ref. Annex 5, Part B-C)_
7.3.5	Il costruttore del veicolo ha messo in atto misure adeguate e proporzionate per garantire che (se previsti) sul tipo di veicolo siano presenti ambienti dedicati per conservare e far funzionare di software, servizi, applicazioni o dati post-vendita. _The vehicle manufacturer has put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data._		□2 □1 □0 Vedi allegato XXYY _See annex XXYY_
7.3.6	Il costruttore del veicolo ha effettuato, prima dell'omologazione, prove adeguate e sufficienti per verificare l'efficacia delle misure di sicurezza attuate. _The vehicle manufacturer has performed, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented._		□2 □1 □0 Vedi allegato XXYY _See annex XXYY_
7.3.7	Il costruttore, per il tipo di veicolo in questione: a) ha rilevato e prevenuto gli attacchi informatici; b) ha potenziato la sua capacità di monitoraggio; c) dispone di capacità di trattamento dei dati che consentano di analizzare gli attacchi informatici. _The vehicle manufacturer, for the vehicle type:_ _(a) has detected and prevented cyber-attacks;_ _(b) has supported the monitoring capability;_ _(c) provides data forensic capability to enable analysis of attempted or successful cyber-attacks._		□2 □1 □0 Vedi allegato XXYY _See annex XXYY_
7.3.8	I moduli crittografici utilizzati ai fini del presente regolamento sono in linea con le norme concordate. Se i moduli crittografici utilizzati non sono in linea con le norme concordate, il costruttore del veicolo ne ha giustificato l'uso.		□2 □1 □0

	Cryptographic modules used for the purpose of this Regulation are in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer has justified their use.		Vedi allegato XXYY *See annex XXYY*
	Totale punteggio / T*otal score*		
	Media / *Average*		

Criteri di valutazione/ Evaluation criteria

Le valutazioni si basano su tre livelli: / *Evaluations are based on three level :*
2 – esiste ed è operante; / *it exists and is operational;*
1 – esiste ma incompleto/non documentato ma operante/operante saltuariamente; / *it exists but incomplete/undocumented but operating/operating occasionally;*
0 – non esiste/inoperante. / *does not exist/operates.*

A conclusione della stesura del presente verbale di verifica la valutazione finale del Costruttore sarà:
At the conclusion of the preparation of this Verification Report, the Builder's final evaluation will be:

DI IDONEITA' se sono verificate entrambe le condizioni seguenti: / *ELIGIBLE if both of the following conditions are met:*
- assenza di "ZERO": / *absence of "ZERO":* N=0
- media M ottenuta: / *average M obtained:* 1,7 ≤ M ≤ 2

DI NON IDONEITA' se si verifica anche solo una delle seguenti condizioni: / *NOT ELIGIBLE if only of the following condition is met:*
- numero di "ZERO": / *number of "ZERO":* N > 0
- media M ottenuta: / *average M obtained:* M < 1,7

d) La quantità delle fotografie scattate durante le prove è a discrezione dell'autorità di omologazione. Nelle prove virtuali, le fotografie possono essere sostituite da stampe di schermate o altri elementi probanti adeguati: **SI/NO/N.A.**

The number of photographs taken during the tests at the discretion of the approval authority. In virtual tests, photographs they may be replaced by prints of screens or other appropriate external evidence: ***YES/NO/N.A.***

OSSERVAZIONI / *OBSERVATIONS* ***N.D.***

CONCLUSIONI E PARERI / ***CONCLUSIONS AND OPINIONS***

- Conclusioni generali delle prove per il sistema, il componente o l'entità tecnica indipendente sottoposto a prova e rappresentativo/a del tipo da omologare:
  Overall test conclusions for the system, component or separate technical unit in the test report that was representative in terms of the type to be approved:

  Sulla base dei criteri di valutazione stabiliti, i veicoli sono conformi alle prescrizioni della norma richiamata in oggetto.

  Based on the established evaluation criteria , the vehicles are comply with the requirements of the provision referred to in item.

- Pareri o interpretazioni inclusi in questo verbale di prova.
  Opinions and interpretations included in this test report.

Rapporto di prova concluso il **00/00/0000**.
Test report concluded on

IL FUNZIONARIO DEL SERVIZIO TECNICO

(dott. ing. ___________________)

VISTO
IL DIRETTORE DEL DERVIZIO TECNICO

(dott. ing. ____________________)